COURSE CONTENT

DATABASE SECURITY								
VIII Semester:CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
2486653	**Foundation**	3	0	0	3	40	60	100
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 45**		
Prerequisites: Data Base Management Systems, Operating Systems.								

Course Overview:

The course provides a comprehensive understanding of security principles, mechanisms, and practices required to protect database systems in modern computing environments. It introduces fundamental concepts of confidentiality, integrity, availability, authentication, authorization, and access control as applied to databases. Students learn how to analyze database vulnerabilities, evaluate risks, and implement appropriate countermeasures.

The course covers essential topics including security models, user privilege management, role-based access control, secure database design, SQL injection prevention, encryption techniques, auditing, backup and recovery strategies, and compliance requirements. Emphasis is placed on understanding real-world threats, secure configuration practices, and defensive techniques used in both centralized and distributed database systems.

Through a combination of theoretical concepts, case studies, and practical exercises, students gain the ability to assess database security posture, identify potential attack vectors, implement security controls, and ensure data protection in alignment with organizational and regulatory standards. The course equips learners with the skills required to design and maintain robust and secure database systems in enterprise environments.

Course Objectives:

1. the fundamental principles of database security, including confidentiality, integrity, availability, authentication, and authorization.
2. the ability to identify database vulnerabilities, security threats, and attack vectors in centralized and distributed database environments.
3. students with the knowledge to apply security models, access control mechanisms, and secure database design principles.
4. learners to implement protective measures such as encryption, auditing, backup, recovery, and intrusion prevention techniques.
5. the capability to evaluate, monitor, and improve the security posture of database systems in compliance with organizational and regulatory requirements.

Course Outcomes: After Completion of the Course, Students should be able to

CO No	Course Outcomes
CO1	Explain the fundamental concepts of database security, threats, and security requirements.
CO2	Analyze vulnerabilities, risks, and attack vectors affecting database systems.
CO3	Apply security models, authentication methods, and access control mechanisms to protect database resources.
CO4	Implement encryption techniques, auditing processes, and secure configuration practices for safeguarding data.
CO5	Evaluate the security posture of database systems and propose appropriate defensive measures aligned with regulatory and organizational policies.

UNIT - I:

Security Architecture: Introduction, Security, Information Systems, Database Management Systems,Information Security,. Information Security Architecture, Database Security, Asset Types and their values, Security Methods.

Operating System Security Fundamentals: Operating System (OS) Overview, Operating System Security Environment, Components of an OS Security Environment, Authentication Methods, User Administration, Password Policies, Vulnerabilities of OS, E-Mail Security.

UNIT - II: Administration of Users: Introduction, Documentation of User Administration, OS Authentication,Creating users, Creating a SQL Server Users, Removing Users, Modifying Users, Default Users,Remote Users, Database Links, Linked Servers, Remote Servers, Practices for Administrators and Managers. Best Practices.

UNIT - III: Profiles, Password Policies, Privileges and Roles: Introduction, Defining and Using Profiles,Designing and Implementing Password Policies, Granting and Revoking User Privileges, Creating Assigning and Revoking User Roles. Best Practices.

UNIT - IV: **Database Application Security Models–** Introduction, Types of Users, Security Models- Types of users, access matrix model, access modes model, commonly used application types. Classes of access control: Discretionary access control (DAC), Mandatory access control (MAC) and Role based Access control (RBAC); Application Types, Application Security Models, Data Encryption, Pharmacy Application.

UNIT - V: Virtual Private Databases- Introduction, Overview of Virtual Private Databases (VPD), Implementing a VPD Using Views, Implementing a VPD Using Application Context in Oracle, Implementing Oracle VPD, Viewing VPD Policies and Application Contexts, Using Policy Manager, Implementing Row and Column level Security with SQL Server.

TEXT BOOKS:

1) Database Security and Auditing: Protecting Data Integrity and Accessibility – Hassan A.Afyouni - Cengage Learning.

REFERENCE BOOKS:

1) Silvano Castano, Fugini, Martella, Samarati, Database Security, Addison Wesley, 1994.
2)M. Gertz, S. Jajodia, Handbook of Database Security, Springer, 2008.

ELECTRONIC RESOURCES:

1.https://www.geeksforgeeks.org/dbms/challenges-of-database-security-in-dbms/

2. .https://docs.oracle.com/cd/B28359_01/server.111/b28318/security.htm?utm_source=chatgpt.com
3. https://www.paloaltonetworks.com/cyberpedia/database-security?utm_source=chatgpt.com
4. https://softpanorama.org/DB/db_security.shtml?utm_source=chatgpt.com
5. https://link.springer.com/chapter/10.1007/978-981-19-3032-4_5?utm_source=chatgpt.com

MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. E-Learning Readiness Videos (ELRV)